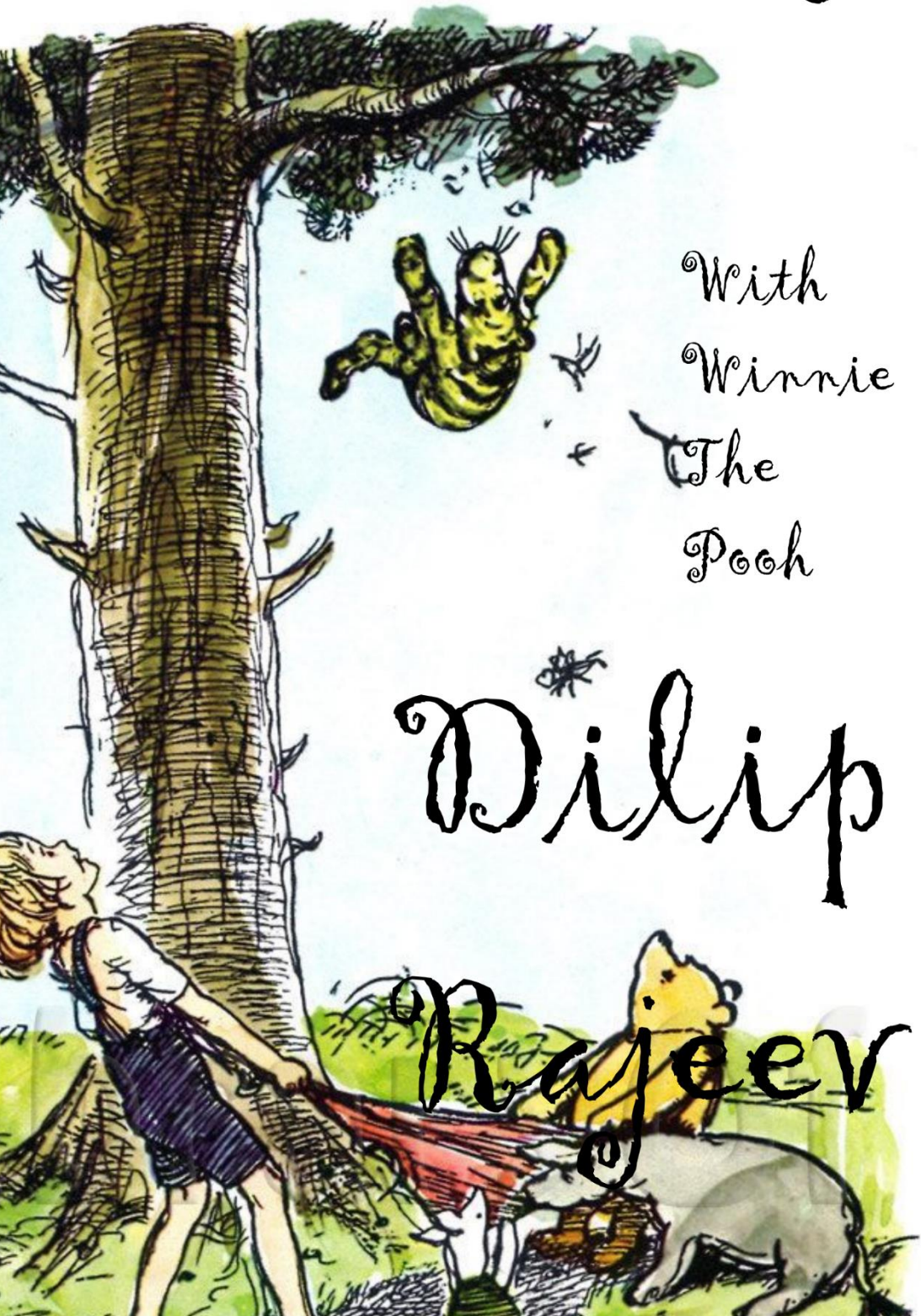
Mathematical Musings



With Winnie The Pooh

Dilip Rajeev

Mathematical Musings

With Winnie the Pooh

DILIP RAJEEV

ISBN:

1

"Did you ever think about why the natural numbers should have an ordering?"

"No," replied, Pooh,

"They just seem kind of well ordered."

" I think there ought be some kind of geometry to what we describe as the Natural numbers. We feel something with a geometry that restricts it to the ordering sense, a geometry upon geometry."

The natural numbers form a system, a geometric structure. Within a number artifact is the entry to the higher number. A center, expanding into a higher space, much as the symbol < suggests.

II. Thus if the 0 artifact has a property, and we find that the artifact N's having the property evolves into the N+1 artifact, then the whole set of natural numbers share that property. This idea is in the principle of Mathematical Induction.

The well ordering principle says every non-empty set of positive integers has a least element. This idea can go into proving that if the ideas described in II, hold for a system – that, " 0 artifact has a property, and we find that the artifact N's having the property evolves into the N+1 artifact" then the whole set of Natural Numbers may be associated with that property. If it were not so, we could assume there exists a non empty set- all of whose elements go without that property. The least element, L, of the set is not zero, as II says otherwise. L-1 therefore does not belong to the set, and has the property, but by II, L also ought have the property. An absurdity – arising from our assumption that such a non-empty set exists.

2

"Have you studied vectors?"

"No," replied Winnie.

"Hear me out, anyway."

If you think the world is a mathematical object, O, and the way it is going to alter in the next time step is O1, both of which would be vectors.. And if you would also assume just from O and O1, every future state of the world is determined, we will do well to study change patterns of [O,O1] to find out the way the world evolves.

Because the path of evolution of the world is entirely determined in that view, there is an ideal path along which the world evolves.

A something adds up minimally along such a path. Why? Because it is an optimal or ideal path.

A function of [O,O1], accumulates ideally along such a path, A bit like if you were to walk to the honey jar, each step you take would be such that the distance sum from the honey jar would be minimal over time.

3

"But what is a vector," asked Winnie.

"Ah." I replied.

The word vector has something to do with what weighs, carries, veh, like the wind, like the thought holding an idea. The awareness holding the world. Well, mathematically it is just an object obeying a few laws.

"Laws," Winne asked with a bit of surprise. There aren't a lot of that found in the woods.

The awareness processes the world, it holds it in itself, and the world is thus the awareness. The vector is the object the awareness holds, and the mathematical form of it is the vector.

4

"Are pebbles of the same color the same," I asked Winnie.

"Obviously they are all different pebbles"

We will assume two pebbles are in a equivalence relationship if they have the same color. So in a box of pebbles, pebbles in a equivalence relationship fall into disjoint sets – sets that do not overlap.

Same color is an equivalence relation Because, in such a relation, if A is related to B, B is related to A, and A is related to itself, and also, if A is related to B, and B is related to C, then A is related to C.

5

“What divides a forest?”

“A stream,” says Winnie.

The same remainder on division by an integer N, is an equivalence relation, and it takes all integers into a set of boxes.

If we were to use same remainder on division by 4, the numbers would all go into boxes we label, based on the remainder, [0],[1],[2],[3].

It turns out that to find out which box any number belonging box [0] added with any number belonging to box [2] goes, we could just add the box labels themselves. Add any number from [0] with any number from [2], it would be in box [0+2]. The same idea holds for multiplication, 5 belongs in [1] and 7 in [3], and so 7*5=35 would belong in box [3].

6

“What is a forest?”

“Just a lot of trees,” says Winnie.

Trees may be different, but to express the idea, the underlying notion of “tree” were taken out. That’s a kind of abstraction.

We saw that the same color relation divided marbles into disjoint sets. And we abstracted out what made the same color relationship do that - its equivalence relation properties.

Having abstracted it out, we can study equivalence relationships in a broad sense.

7

“W adds?”

“Numbers?” wondered Tigger.

“Anything under the sun,” Winne said, ‘I can add another bottle of honey to the shelf,”.

We formed labels for remainder classes [0] [1], etc. And it turned out we could add the labels themselves in a meaningful way. If the labels were formed on division by 4, [2] and [2] would add to give [0]. There is addition going on but how similar is it to addition of usual integers?

Similarly, in the example just given, [2] multiplied by [2] would give [0]. That’s strange and unlike usual numbers. Among usual numbers one has to multiply by a zero label to get a zero, and that zero label is unique. In our new system of kind of number like things, [2].[2]=[0], seems that makes somewhat weird and different from the usual sense of integer domains – where two non-zero numbers do not multiply to a zero .

If n were prime, instead of 4, then either a or b would need to be 0 for [a][b]=[0], which may easily be observed from that a prime number has no two factors less than itself.

And if n were prime, every [a] would have a multiplicative inverse [b] such that [a][b]=1.

If the labels were formed by division on 4, we term the labels [0],[1],[2],[3].. along with the idea that we can perform addition and multiplication on them, a number system with the name Z/nZ. Just as Complex numbers are a number system with the label C.

Observing these properties we say that Z/nZ, forms a field if n is prime. A field is any structure that obeys a set of rules which makes it a field – just as existence of a multiplicative inverse, that multiplication distributes over addition, etc. Real numbers and complex numbers form a field. One may abstractly study properties of all fields by studying what the laws that make a field entails, and thus discover properties that hold for R, C, Z/pZ, all alike.

8

“A field is a group”

“Whatever, it is math jargon,” said Pooh.

We will get to this afterwards with a greater picture. But, for now remember there are things that can form what obeys the rules of a mathematical field – like real numbers, complex numbers and so on.

A field is in fact a group – under both multiplication{the field without the [0]} and addition. A group is a

term given to, again, mathematical objects that obey a set of rules that form a group.

Now, as Z/pZ is a field, its elements G={1,2..(p-1)} also form a group under the new kind of multiplication.

If [a] is an element of G, it being an element of a group, {[a],[a]^2…[a]^k=[1]}, all together form elements of a subgroup of G. There is a theorem that holds for all groups that the number of elements of a group is an integer multiple of the number of elements of any of its subgroups. So, k divides p-1, and it holds that [a]^(p-1)=a^(k*n)=(a^k)^n which is [1]^n, which is 1.

This is Fermat's "little" theorem, if [a] is an element of Z/pZ, [a]^(p-1) =[1].

8

“The Greatest Common Divisor!”

“That sounds like something that would divide anything,” said Winnie.

Well, the greatest common divisor of any two numbers is the largest number that divides it both.

Assume a number were a strip – the number 4 would be a strip of 4 units, with markings indicating the end of each unit. And number 12 a similar strip, of 12 units length.

We put the strip 4 upon the strip 12, and it overlaps revealing 8 units.

Its easy to see as the GCD, the greatest common divisor divides both the numbers, it divides their difference too, the 8 units revealed in the previous case.

It is easy to see that this holds for anu two numbers A and B. And not just that - the GCD would divide the difference between any two integer multiples of A and B. That is to say (kA- gB) would be divisible by the GCD of A and B.

A bit of visualization would lead you to that the GCD of A and B, is the least number we can get of the form (kA- gB), as the GCD divides all numbers of that form.

Now, assume A and B are relatively prime. By definition, A and B are said to be relatively prime, if GCD of A and B, is 1. That is to say, if A and B are prime there exists two integers k, g such that (kA- gB)=1, or, if we say f is the negative version of g, two integers k and f such that (kA+fB)=1,

A fancy way of writing, GCD of A and B, is GCD(A,B).

9

“I will describe the way a secret message can be sent . Don’t bother if you don’t understand.”

“Hiding the way you hide a secret is a good way to keep a secret,” the Piglet observed.

Well, first we need to find two large primes. Fermat’s last theorem allows us to say if a number n is not prime, we run tests on random numbers in the Z/nZ, world to find if a contradiction to [a]^(n-1) =[1] is found. If a number is not prime a contradiction would quickly arise as one samples random numbers in that sample space, on the test.

If a number is found to be not prime, one can move to the next random guess, and perform the test. With a few refinements we can verify if a number is a prime with a good degree of efficiency. Primes are scattered around at around 1/ln(n) frequency as n gets large.

Once we find two large primes, p and q,

The product of two primes p and q, $N=p*q$, may be published without the risk of anyone figuring out p or q. As there is no efficient way known in usual computing, to factor a large number N. Quantum computing is a different story, but there are no quantum computers in the woods, yet.

Now, there are two things we need - a magic key to lock the secret in, which fancy people call the encryption key, E, and, a magic key to unlock the secret out, which fancy people call the decryption key, D.

Assume K is(p-1)(q-1). "Why do we chose K as that fancy number?", Winne asked. "Well.. you will see that. But here is a hint, Fermat discovered [a]^(p-1) is 1 in

the Z/pN world."

"I guess we could make stuff disappear into a 1, if we get to multiply by that," said the donkey, in a sudden stroke of genius.

"Make what disappear?" I asked the donkey.

By the time I asked the question, the muses had abandoned Donkey to his own devices, and Donkey had no answer.

"Well, it could be to make the cover we put on the secret message disappear, " I hinted. "Sounds reasonable," said Donkey, in a sober tone.

Back to what I were saying,

Assume K =(p-1)(q-1), where p and q were two large prime

numbers we found.

We find a number D, that is relatively prime to K. That is, from what I said in the previous section, there exists two integers E and G such that E.D-G.K=1,

In other words E.D =G.K+1, that is to say on division by K, E.D leaves a remainder of 1.

In yet other words, [E] and [D] are multiplicative inverses in the Z/KZ world. [E] multiplied by [D] in that world is a [1].

We take E for the encryption key – the secret lock, and D for the decryption key, the unlock.

Assume I need to receive a secret message from a base in Antarctica, I send them the numbers N, and D.

The secret message they can send me now, is any number in the Z/NZ world.

Assume that number is [S], the recipient sends me [S]^E in the Z/NZ world. I take [S] ^E and raise it by D, ([S]^E)^D, which turns out to be [S].

Because only I have the Secret

Decryption Key

D, and nobody else, only I can use that procedure to uncover [S], the original message, from ([S]^E).

Now, why would this magic occur?

Why is that ([S]^E)^D=

[S]^(ED)=[S] in the Z/NZ world.

To see this, we observe first that if numbers S^(ED) and S take on the same label in the Z/pZ world; and that they also taken on the label the Z/qZ world

then it they take on the same labels in the Z/NZ world.

The previous paragraph says (S^(ED) -S) being divisible by both the primes p and q says it is it

is divisible by N=p*q. That is, [S]^(ED)=[S] in the Z/NZ world.

So, we now set out to demonstrate that, S^(ED) and S take on the same label in the Z/pZ world.

And the same argument would apply to the $\mathbb{Z}/q\mathbb{Z}$ world, without any difference.

Now, remember that In the Z/KZ world (D*E) is [1]. They were selected to be inverses of each other by multiplication, in that world. That is to say,

D*E=[1]=a*K+1=a(p-1)(q-1)+1.

Lets find out what S becomes in the Z/pZ when raised by (D.E).

S^(D.E)=S^(a(p-1)(q-1)+1)=S * S^(a(p-1)(q-1))

But S^(a(p-1)(q-1)) is (S^(p-1))^(a*(q-1)) and by Fermat's little theories, (S^(p-1)) is [1] in the Z/pZ world.

Thus, S^(D.E) and S have the same labels in the Z/pZ world and by the exact same argument, it is so in the Z/qZ world.

Thus, as we have shown, since S^(D.E) - S is [0] in both the Z/pZ and Z/qZ worlds, and the same holds in Z/NZ,

So,

$$[S]^{(D.E)} = [S] \text{ in the } Z/nZ \text{ world.}$$

In short, we make a encryption key E, and decryption key D, based on two large primes, and N which is the product of the two primes. To someone

who wants to send us a secret, we send the number N, and the

number E.

The recipient sends us the secret which has to be a number in the Z/NZ world.

Assume that number is S<N, and in the Z/NZ world is [S]. If he or she were to send us [S], anyone could

intercept the letter and read the message. Instead of sending us [S], it is wrapped up in a secret cover by making it [S]^E, in the Z/NZ world, and then sent to us. On getting [S]^E, we do ([S]^E)^D in the Z/NZ world, which unveils the original message [S].

"Why can't I divide 5 with 3!" asked Piglet, playing with pebbles.

"Because nothing of the sort exists," said Donkey.

Winnie were in the next room preparing breakfast for all three of us. "We've got 3 toasts and 5 bottles of honey you can have with it."

There were silence in the room. Donkey seemed to be pondering his existence.

"Donkey, you were right," "Five divided by three doesn't exist in the world of pebbles," I said.

Division is a kind of operation we can perform on numbers. In the world of whole numbers, or of integers, division turns up things that are out of the world. Things like five divided by three are nowhere found in the world of integers of whole numbers.

So we say, the Integers and whole numbers are not closed under the operation of division.

"If something out of the world turned up every time we divided, it would be fun," Piglet observed.

Well, mathematicians are often strange and boring people. They enjoy studying closed systems. And sets of things and operations on those things, which turn up things within that set itself.

Integers are closed under the operation of addition, for instance. If we added two integers, we would get an integer.

“What other things can you discover about integers!”

Well, integers are closed under addition. In adding any 3 integers, a, b, c, we find the order in which we add them doesn’t matter that is (a+b)+c is a+(b+c). This rule is called associativity under addition.

“Does that also mean I could replace b with say, e+(f+g), and then shift around all the brackets like the rule would allow?”, asked Piglet.

“Yep.”

In fact, if you play around with the idea, you will see that the associativity for three numbers imply you can put brackets anywhere in a long list of numbers being added, The order in which you sum them up doesn’t matter.

Then, we discover the existence of an identity under addition. There is a number which if you added

to any other number in the Integer world, you get the same number.

"The Zero," said Donkey.

"That's Right!"

In the world of integers we have additive inverses for every number. By adding -3 to 3, we get zero. So -3 is the additive inverse of 3.

We have commutati

vity for addition, a+b is the same as b+a.

And there is associativity for multiplication as well. (A*B)*C is the same as A*(B*C).

There is a multiplicative identity, 1.

A multiplicative

identity is something that works in a way as the expression below, on any element A,

$1*A=A*1=A$

And multiplication distributes over addition. A(B+C) is AB+AC. Further, (B+C)A is BA+CA.

"Did you know the Ringa-Ringa Roses song is about a dark and ghostly time when everybody died sneezing?" asked Winnie.

"And did they become sneezing ghosts?" asked Piglet wide eyed

"Ghost stories under the moonlight are not fun," Tigger whispered to himself.

Well.. the properties of integers we discovered the other day, all put together form properties of what we will give the name, a Ring.

So that we can study all worlds where those ideas hold.

"One ring to rule them all?" asked Tigger in a trembling voice.

"Yep."

"What would be a world of our own like?" asked Winnie.

I were lost in the thought as we walked down the stream, under the moon. "A mathematical world?"

We will build the smallest Ring ever. It has just one element. A something we will give the name [0]. It obeys the rules [0]+[0]=[0] and [0].[0]=[0]

This idea we have built is the smallest Ring possible. It satisfies all the rules a thing needs to satisfy to be a Ring. A Ring R made of the set R, and the operations + and . is denoted by (R,+,.).

Here the set R={[0]}

This ring we call the trivial Ring.

"And what happens in worlds that are rings?", Winnie asked.

"Would there be Fairies, Wizards and Dragons?"

"Well, there will have to be a 0 and a 1", I answered, trying not to disappoint.

"Well.. for one.. There can only be one 0 and one 1 element in such a world," I said.

As we have seen already, Z is a ring. Z/nZ forms a ring, for all n greater than zero. The set of n*n matrices form rings, if its entries are real numbers. For instance, the set of 2*2 matrices obey all rules we identified for a Ring, - on adding two such matrices, we have a 2*2 matrix, thus closure, we have associativity of addition, and so on – which you could experiment and discover on own. In fact the elements of the matrix needn't be real numbers, it could be from any world that is a Ring – real numbers happen to be one such world.. So, the set of all 5*5 matrices, with entries made of 2*2 matrices of integers is a ring.

Polynomials form rings, if their coefficients are elements

of a ring. Polynomials are things, if you remember from high school, that look like a +a1 x+ a2 x^2.. +an x^n.

In matrices form a Ring, it is an easy guess that the set of all linear transformations on a vector space form a ring.

In all these worlds, all general properties we discover for rings hold true.

"But in the Trivial Ring, there were only one element, a [0]" said Winnie.

In the Trivial Ring, [0] were playing the role of both [1] and [0]. So, in a way, there were both a [1] and a [0]. [0] were just a label we selected. We could as easily have labeled it [a] and made up the same rules [a]*[a]=[a] and [a]+[a]=a.

And let's set to discovering a few properties of rings. One idea we see is that there cannot be two additive identities, 0s, in any ring. Well, lets assume [01] and [02] are two such identities. Associativity tells us that we could add either [01] or [02], to either side of a ring element to get the same thing.

Then in the Ring worlds, [01]+[02] is the same as [01] and is also the same as [02]. Thus, we can say [01]=[01]+[02]=[02]. So, both of them are the same element. This holds in all the Ring worlds. See, how easily we proved this for all the fancy ring worlds out there?

“How many 1s can exist in the world?”, asked Winnie.

“Well, I assume by 1 you mean the multiplicative identity”
“Yep.”

“If there were two such, [1] and [1’], what does this say?

[1]=[1][1’]=[1’], ” I asked

“That [1] and [1’] need to be the same thing!” said Winnie.

"One way to make things disappear is magic"

"And another way?" asked Winnie.

"The additive inverse"

In the world of integers, it seems ever number has its additive inverse, which is unique. 4 has for its additive inverse – 4

We will try to find out if it is so in any ring. Is the additive inverse unique?

We could just fool around with the idea a bit and see that the additive inverse can be added to either side of an element A. Assume A has two inverses I1 and I2

I1+A+I2 can be by the associative property read in two ways. And what do those two ways turn up?

In all worlds that are Rings we can do this neat trick. Which is to make the same thing on either side of an equality of two addition expressions disappear.

If a+b= a+c, we could make 'a' disappear and say b=c, in that Ring.

Well, this phenomenon appears from the rules for Rings, which mathematicians also call Ring axioms, a fancy word for fixed laws, things assumed to be true and so on.

This is because b can be written as 0+b, which is (-a+a) +b , moving the brackets around we get- a +(a+b), which the assumption a+b=a+c, allows us to write as -a +(a+c). Now again moving the brackets around, we get (-a+a)+c, which is c.

Multiplication by the additive identity, zero entails a zero, in any Ring. A(0)=A(0+0), A0=A0+A0. We then add zero to either side of the expression A0+0=A.0+A.0+0. Making A.0 disappear from each side, we get 0= A.0+0. As 0 is the additive identity, we then say A.0=0